Joint Statement on the PageUp Limited Data Incident

Australian Government
Office of the Australian Information Commissioner

ACSC AUSTRALIAN CYBER SECURITY CENTRE

IDCARE

18 June 2018

On Friday 1 June 2018 PageUp Limited, an online recruitment services organisation, notified their customers about a data incident in relation to the integrity of their systems – proactively informing of a possible breach.

PageUp self-identified suspicious activity on its network and undertook immediate actions to investigate and contain the incident. PageUp notified their corporate customers and the Australian Cyber Security Centre (ACSC) of the issue, enabling the ACSC to quickly assess the incident and support PageUp in their response. In line with the new Notifiable Data Breaches (NDB) scheme, PageUp also notified the Office of the Australian Information Commissioner (OAIC). PageUp is in contact with its corporate clients to facilitate notification to individuals.

Although investigations are ongoing, PageUp believes that certain information pertaining to staff members, applicants and referees was *accessed* by an unauthorised third party. Further information about the types of information affected can be found at **PageUp's website** <https://www.pageuppeople.com/unauthorised-activity-on-it-system/>. PageUp has advised that no employment contracts, applicant resumes, Australian tax file numbers, credit card information or bank account information were affected.

While recognising that investigations are ongoing and that the situation may therefore change, the ACSC emphasises that there is a significant distinction between information being *accessed* (which means there has been a systems breach) and information being *exfiltrated* by the offender. In other words, no Australian information may actually have been stolen.

IDCARE is Australia's expert community identity and cyber support service and has been working with impacted organisations and members of the community in relation to this incident.

Dave Lacey, Managing Director, IDCARE says:

> *'Whilst it is important to acknowledge that breached personal information impacts people in different ways, based on investigations undertaken to date by PageUp, at this point IDCARE*

> *assesses that the direct risk of identity theft is unlikely. Identity thieves typically require other forms of personal information to successfully manipulate this type of data, such as driver licence, passport, and account details, in order to obtain credit in a person's name or related acts of impersonation.*
>
> *IDCARE assesses that there are other risks that are likely to be more relevant to impacted individuals, including the possibility of phishing emails, telephone scam calls, and specific risks to individuals concerned about their contact information, physical address, and employment details (and applications) becoming known to third parties.'*

PageUp has provided public updates, and has held multiple corporate customer information sessions facilitated through the ACSC to help keep affected organisations informed.

Alastair MacGibbon, Head of the Australian Cyber Security Centre and National Cyber Security Adviser says:

> *'PageUp has committed to advising impacted organisations and individuals if there are any new findings to arise as they complete their investigations. PageUp has demonstrated a commendable level of transparency in how they've communicated about, and responded to, this incident: they came forward quickly and engaged openly with affected organisations.'*

In this era of widespread cyber security threats, organisations must be prepared to prevent, detect and respond to incidents, to engage with relevant authorities and to provide timely and open communications to those affected.

Consistent with previous advice, the OAIC, ACSC and IDCARE jointly recommend that individuals who believe their information may be held by one or more of the organisations impacted consider the following measures:

- Immediately change passwords that may be the same as the one used during the recruitment process undertaken with impacted organisations.
- Regularly change passwords and make them hard to guess.
- Be wary of phishing emails by reviewing the sender of the email and be cautious of links and attachments – if in doubt, make your own enquiries with the organisation and individual concerned using other means.
- Avoid telephone scammers – good organisations don't call you and then ask for your details – if in doubt, finish the call and do your own research by finding an alternative contact point and checking to see if the real organisation did call.

For further information on how to protect your identity and respond to identity concerns please visit the **OAIC's data breach guidance** </individuals/data-breach-guidance> for individuals and **IDCARE's Learning Centre** <https://www.idcare.org/learning-centre>.

For general easy-to-use information for the public and small to medium businesses, visit the Australian Cyber Security Centre's **Stay Smart Online** <https://www.staysmartonline.gov.au/> website.

To report a cyber security incident visit the **Australian Cyber Security Centre's** <https://acsc.gov.au/incident.html> website.

To notify the Office of the Australian Information Commissioner of an eligible data breach involving personal information, organisations should use the the **OAIC's Notifiable Data Breach form** </privacy-law/privacy-act/notifiable-data-breaches-scheme#how-to-notify>.

Alastair MacGibbon
Head of the Australian Cyber Security Centre and National Cyber Security Adviser

Angelene Falk
Acting Australian Information Commissioner and acting Australian Privacy Commissioner

Dave Lacey
Managing Director, IDCARE